

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

BRENDAN GEE,

Plaintiff,

v.

DUANE HINRICHS, JR. et al.,

Defendants.

CASE NO. C23-5695-KKE

ORDER GRANTING AGREEMENT
REGARDING DISCOVERY OF
ELECTRONICALLY STORED
INFORMATION

The parties hereby stipulate to the following provisions regarding the discovery of electronically stored information (“ESI”) in this matter:

A. General Principles

1. An attorney’s zealous representation of a client is not compromised by conducting discovery in a cooperative manner. The failure of counsel or the parties to litigation to cooperate in facilitating and reasonably limiting discovery requests and responses raises litigation costs and contributes to the risk of sanctions.

2. As provided in LCR 26(f), the proportionality standard set forth in Fed. R. Civ. P. 26(b)(1) must be applied in each case when formulating a discovery plan. To further the application of the proportionality standard in discovery, requests for production of ESI and related responses

1 should be reasonably targeted, clear, and as specific as possible. This agreement is intended to
2 assist the parties in identifying relevant, responsive information that has been stored electronically
3 and is proportional to the needs of the case. The agreement does not supplant the parties'
4 obligations to comply with Fed. R. Civ. P. 34.

5 **B. ESI Disclosures**

6 Within 30 days of entry of this Order, or at a later time if agreed to by the parties, each
7 party shall disclose:

8 1. Custodians. The custodians most likely to have discoverable ESI in their
9 possession, custody, or control. The custodians shall be identified by name, title, connection to the
10 instant litigation, and the type of the information under the custodian's control.

11 2. Non-custodial Data Sources. A list of non-custodial data sources (*e.g.*, shared
12 drives, servers), if any, likely to contain discoverable ESI.

13 3. Third-Party Data Sources. A list of third-party data sources, if any, likely to contain
14 discoverable ESI (*e.g.*, third-party email providers, mobile device providers, cloud storage) and,
15 for each such source, the extent to which a party is (or is not) able to preserve information stored
16 in the third-party data source.

17 4. Inaccessible Data. A list of data sources, if any, likely to contain discoverable ESI
18 (by type, date, custodian, electronic system or other criteria sufficient to specifically identify the
19 data source) that a party asserts is not reasonably accessible under Fed. R. Civ. P. 26(b)(2)(B).

20 **C. ESI Discovery Procedures**

21 1. On-site inspection of electronic media. Such an inspection shall not be required
22 absent a demonstration by the requesting party of specific need and good cause or by agreement
23 of the parties.
24

1 2. Search methodology. The parties shall timely confer to attempt to reach agreement
2 on appropriate search terms and queries, file type and date restrictions, data sources (including
3 custodians), and other appropriate computer- or technology-aided methodologies, before any such
4 effort is undertaken. The parties shall continue to cooperate in revising the appropriateness of the
5 search methodology.

6 a. Prior to running searches:

7 i. The producing party shall disclose the data sources (including
8 custodians), search terms and queries, any file type and date restrictions, and any other
9 methodology that it proposes to use to locate ESI likely to contain responsive and discoverable
10 information. The producing party may provide unique hit counts for each search query.

11 ii. After disclosure, the parties will engage in a meet and confer
12 process regarding additional terms sought by the non-producing party.

13 iii. The following provisions apply to search terms / queries of the
14 requesting party. Focused terms and queries should be employed; broad terms or queries, such
15 as product and company names, generally should be avoided. A conjunctive combination of
16 multiple words or phrases (*e.g.*, “computer” and “system”) narrows the search and shall count as
17 a single search term. A disjunctive combination of multiple words or phrases (*e.g.*, “computer”
18 or “system”) broadens the search, and thus each word or phrase shall count as a separate search
19 term unless they are variants of the same word. The producing party may identify each search
20 term or query returning overbroad results demonstrating the overbroad results and a counter
21 proposal correcting the overbroad search or query.

22 c. Upon reasonable request, a party shall disclose information relating to
23 network design, the types of databases, database dictionaries, the access control list and security
24

1 access logs and rights of individuals to access the system and specific files and applications, the
2 ESI document retention policy, organizational chart for information systems personnel, or the
3 backup and systems recovery routines, including, but not limited to, tape rotation and
4 destruction/overwrite policy.

5 3. Format.

6 a. ESI will be produced to the requesting party with searchable text, in a
7 format to be decided between the parties. Acceptable formats include, but are not limited to, native
8 files, multi-page TIFFs (with a companion OCR or extracted text file), single-page TIFFs (only
9 with load files for e-discovery software that includes metadata fields identifying natural document
10 breaks and also includes companion OCR and/or extracted text files), and searchable PDF.

11 b. Unless otherwise agreed to by the parties, files that are not easily converted
12 to image format, such as spreadsheet, database, and drawing files, will be produced in native
13 format.

14 c. Each document image file shall be named with a unique number (Bates
15 Number). File names should not be more than twenty characters long or contain spaces. When a
16 text-searchable image file is produced, the producing party must preserve the integrity of the
17 underlying ESI, *i.e.*, the original formatting, the metadata (as noted below) and, where applicable,
18 the revision history.

19 d. If a document is more than one page, the unitization of the document and
20 any attachments and/or affixed notes shall be maintained as they existed in the original document.

21 4. De-duplication. The parties may de-duplicate their ESI production across custodial
22 and non-custodial data sources after disclosure to the requesting party, and the duplicate custodian
23
24

1 information removed during the de-duplication process tracked in a duplicate/other custodian field
2 in the database load file.

3 5. Email Threading. The parties may use analytics technology to identify email
4 threads and need only produce the unique most inclusive copy and related family members and
5 may exclude lesser inclusive copies. Upon reasonable request, the producing party will produce a
6 less inclusive copy.

7 6. Metadata fields. If the requesting party seeks metadata, the parties agree that only
8 the following metadata fields need be produced, and only to the extent it is reasonably accessible
9 and non-privileged: document type; custodian and duplicate custodians (or storage location if no
10 custodian); author/from; recipient/to, cc and bcc; title/subject; email subject; file name; file size;
11 file extension; original file path; date and time created, sent, modified and/or received; and hash
12 value. The list of metadata type is intended to be flexible and may be changed by agreement of the
13 parties, particularly in light of advances and changes in technology, vendor, and business practices.

14 **D. Preservation of ESI**

15 The parties acknowledge that they have a common law obligation, as expressed in Fed. R.
16 Civ. P. 37(e), to take reasonable and proportional steps to preserve discoverable information in the
17 party's possession, custody, or control. With respect to preservation of ESI, the parties agree as
18 follows:

19 1. Absent a showing of good cause by the requesting party, the parties shall not be
20 required to modify the procedures used by them in the ordinary course of business to back-up and
21 archive data; provided, however, that the parties shall preserve all discoverable ESI in their
22 possession, custody, or control.

2. The parties will supplement their disclosures in accordance with Fed. R. Civ. P. 26(e) with discoverable ESI responsive to a particular discovery request or mandatory disclosure where that data is created after a disclosure or response is made (unless excluded under Sections (D)(3) or (E)(1)-(2)).

3. Absent a showing of good cause by the requesting party, the following categories of ESI need not be preserved:

- a. Deleted, slack, fragmented, or other data only accessible by forensics.
- b. Random access memory (RAM), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system.
- c. On-line access data such as temporary internet files, history, cache, cookies, and the like.
- d. Data in metadata fields that are frequently updated automatically, such as last-opened dates (see also Section (E)(5)).
- e. Back-up data that are duplicative of data that are more accessible elsewhere.
- f. Server, system or network logs.
- g. Data remaining from systems no longer in use that is unintelligible on the systems in use.
- h. Electronic data (*e.g.*, email, calendars, contact data, and notes) sent to or from mobile devices (*e.g.*, iPhone, iPad, Android devices), provided that a copy of all such electronic data is automatically saved in real time elsewhere (such as on a server, laptop, desktop computer, or “cloud” storage).

E. Privilege

1. A producing party shall create a privilege log of all documents fully withheld from production on the basis of a privilege or protection, unless otherwise agreed or excepted by this Agreement and Order. Privilege logs shall include a unique identification number for each document and the basis for the claim (attorney-client privileged or work-product protection). For ESI, the privilege log may be generated using available metadata, including author/recipient or

1 to/from/cc/bcc names; the subject matter or title; and date created. Should the available metadata
2 provide insufficient information for the purpose of evaluating the privilege claim asserted, the
3 producing party shall include such additional information as required by the Federal Rules of Civil
4 Procedure. Privilege logs will be produced to all other parties no later than 30 days after delivering
5 a production unless an earlier deadline is agreed to by the parties.

6 2. Redactions need not be logged so long as the basis for the redaction is clear on the
7 redacted document.

8 3. With respect to privileged or work-product information generated after the filing of
9 the complaint, parties are not required to include any such information in privilege logs.

10 4. Activities undertaken in compliance with the duty to preserve information are
11 protected from disclosure and discovery under Fed. R. Civ. P. 26(b)(3)(A) and (B).

12 5. Pursuant to Fed. R. Evid. 502(d), the production of any documents, electronically
13 stored information (ESI) or information, whether inadvertent or otherwise, in this proceeding shall
14 not, for the purposes of this proceeding or any other federal or state proceeding, constitute a waiver
15 by the producing party of any privilege applicable to those documents, including the attorney-
16 client privilege, attorney work-product protection, or any other privilege or protection recognized
17 by law. This Order shall be interpreted to provide the maximum protection allowed by Fed. R.
18 Evid. 502(d). The provisions of Fed. R. Evid. 502(b) do not apply. Nothing contained herein is
19 intended to or shall serve to limit a party's right to conduct a review of documents, ESI or
20 information (including metadata) for relevance, responsiveness and/or segregation of privileged
21 and/or protected information before production. Information produced in discovery that is
22 protected as privileged or work product shall be immediately returned to the producing party.

1 DATED: December 20, 2023.

2 Respectfully submitted,

3 /s/ Aaron Elinoff

4 Aaron Elinoff, Esq. (WBSA No. 58949)
NOVO LEGAL GROUP, P.L.L.C.
19309 68th Ave S Suite R-102
5 Kent, WA 98032
T: (303) 335-0250
6 E: aaron@novo-legal.com

7 /s/ Aaron Slade

8 Aaron Slade, Esq.*
NOVO LEGAL GROUP, L.L.C.
4280 Morrison Road
9 Denver, CO 80219
T: (303) 335-0250
10 E: aslade@novo-legal.com

11 *Appearing pro hac vice

12 *Counsel for Plaintiff*

13 /s/ John E. Justice

14 John E. Justice, WSBA No. 23042
P.O. Box 11880
Olympia, WA 98508-1880
15 Tel: (360) 754-3480 Fax: (360) 357-3511
Email: jjustice@lldkb.com

16 *Counsel for Defendants*

ORDER

Based on the foregoing, IT IS SO ORDERED.

Dated this 22nd day of December, 2023.

A handwritten signature in black ink, reading "Kimberly K. Evanson". The signature is written in a cursive style with a large, stylized "K" and "E".

Kimberly K. Evanson
United States District Judge